Senior Service College Fellowship
Civilian Research Project

GENERATING A GLOBAL CYBER CODE OF CONDUCT

BY

LIEUTENANT COLONEL STEVEN R. SCHWEICHLER
United States Army

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04--2011	Civilian Research Paper	

4. TITLE AND SUBTITLE
Generating a Global Cyber Code of Conduct

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LTC Steven R. Schweichler

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Fletcher School of Law and Diplomacy
Tufts University
Medford, MA 02155

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Ave.
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The United States (U.S.) and other nations have become increasingly reliant on digital information and communications systems over the last two decades. The increased technological advances in these systems have revolutionized how nations and populations communicate, making once difficult tasks easier and faster. Disadvantages also emerged with this capability, including the ability to probe and gain access to information by "hacking" into information and communications systems. With this growing cyber security threat, it was not clear if the current rules of engagement were sufficient, or if a new global cyber code of conduct was necessary, to protect U.S. information and communications systems against cyber attacks. The methods used to gather information for this study included research analyzing the current U.S. rules of engagement at the U.S. government, Department of Defense, and military services levels to determine their sufficiency. The current U.S. rules of engagement are not sufficient in protecting the U.S. against cyber security attacks, and it is necessary to implement a global cyber code of conduct to mitigate this growing security threat.

15. SUBJECT TERMS

Cyber, Security, Global, Information, Communications, Threats

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	46	

USAWC CIVILIAN RESEARCH PROJECT

GENERATING A GLOBAL CYBER CODE OF CONDUCT

by

Lieutenant Colonel Steven R. Schweichler
United States Army

Dr. William C. Martel
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Senior Service College Fellowship Program.

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: LTC Steven R. Schweichler

TITLE: Generating a Global Cyber Code of Conduct

FORMAT: Civilian Research Project

DATE: 01 April 2011 WORD COUNT: 9,084 PAGES: 46

KEY TERMS: Cyber, Security, Global, Information, Communications, Threats

CLASSIFICATION: Unclassified

The United States (U.S.) and other nations have become increasingly reliant on digital information and communications systems over the last two decades. The increased technological advances in these systems have revolutionized how nations and populations communicate, making once difficult tasks easier and faster. Disadvantages also emerged with this capability, including the ability to probe and gain access to information by “hacking” into information and communications systems. With this growing cyber security threat, it was not clear if the current rules of engagement were sufficient, or if a new global cyber code of conduct was necessary, to protect U.S. information and communications systems against cyber attacks. The methods used to gather information for this study included research analyzing the current U.S. rules of engagement at the U.S. government, Department of Defense, and military services levels to determine their sufficiency. The current U.S. rules of engagement are not sufficient in protecting the U.S. against cyber security attacks, and it is necessary to implement a global cyber code of conduct to mitigate this growing security threat.

TABLE OF CONTENTS

GENERATING A GLOBAL CYBER CODE OF CONDUCT

In the spring of 2007, the nation state of Estonia experienced first hand that cyber attacks are a real and viable means of conducting warfare. There were no boundaries to this attack with both government and civilian agencies targeted. Many organizations in Estonia fell prey to the attack, including banks, ministries, and multiple media outlets. Most disturbing was the attack on the emergency contact number, and the fact that Estonia had no way to inform the international community they were under attack.[1] Fast forward to the nation state of Georgia in the summer of 2008 where three separate cyber attacks occurred during the months of July and August. Coincidentally, the third attack occurred in conjunction with Russian soldier movements in response to Georgian military operations in South Ossetia. These cyber attacks denied the Georgian government access to their own Websites, virtually causing a communication shutdown.[2]

These cyber attacks on Estonia and Georgia are indicators that cyberspace has become the future battlefield for conducting warfare.[3] Cyber warfare brings new challenges to the international community as nation states become ever more reliant on digital information and communications systems and the trend toward globalization makes the world ever smaller. As nation states analyze the cyber security threat, there are many issues to consider. For instance, the current cyber rules of engagement established by the United States (U.S.) government to protect information and communications systems are several years old, with some as old as a decade. This raises the debate as to whether these rules of engagement are still applicable in

protecting the U.S. against cyber attacks similar to or more sophisticated than those conducted against Estonia and Georgia.

This study analyzes the current U.S. rules of engagement to determine whether they are sufficient to protect the U.S. information and communications systems against new forms of cyber attacks. Understanding the current U.S. rules of engagement, and whether they are flexible enough to withstand the dramatic changes that cyber technology has brought about over the last several decades, is paramount to understanding how to address the mitigation of future U.S. cyber attacks. Once this question is answered, a baseline can be established to aid in determining whether to maintain the status quo in terms of the current rules of engagement, or provide new solutions to protect the U.S. information and communications systems against cyber attacks. One such solution, the establishment of a global cyber code of conduct, will be examined to determine its viability in deterring cyber attacks.

The first section of this study provides an overview of the development of the U.S. information and communications systems over the last two decades, including how the modern cyber domain evolved, how these threats have escalated over the years, and some potential cyber attack scenarios the U.S. could face in the future. The focus of the study will then turn toward the current U.S. rules of engagement from the U.S. President's, Department of Defense (DoD), and military services' perspectives. The final section is a discussion on the inadequacies of the current U.S. rules of engagement in protecting U.S. information and communications systems, and a follow-on discussion promoting the establishment of a global cyber code of conduct.

The scope of this study is limited to several areas to more manageably focus the broad category of cyber security. Although other organizations within the U.S. government address protection of information and communications systems, this study will focus on the U.S. President's guidelines from a DoD perspective, more specifically on the U.S. Army, Navy, and Air Force, since it is the branch of the government specifically charged with defending the nation. In addition, this study will only address cyber attacks as they relate to nation states. Although non-state actors play a role in conducting cyber attacks, for purposes of narrowing the discussion, they will not be addressed in this study.

Background

To adequately assess the effectiveness of the current U.S. cyber rules of engagement, it is important to understand the history of these information and communications systems and how information technology has advanced so rapidly over the last two decades to the modern systems that exist today.[4] This section provides background, including the current types of cyber security threats and how these threats have escalated.

Definitions. Two terms used in this study require clarification, the first of which is "rules of engagement." According to the military use of this term, "rules of engagement" are directives given, by someone considered to have military authority, that establishes a set of circumstances and limitations to which military forces can start or continue to engage an opposing force.[5] The term "code of conduct" is similar to "rules of engagement" in that it also establishes a set of rules for certain circumstances, providing a baseline or standard for the members within a group. However, the term

"code of conduct" goes a step further in that it also addresses cooperation with others outside of the organization.[6] For the purpose of this study, the distinction will be made between these two terms in that "rules of engagement" are a set of established rules focused internally on the members of an organization, whereas "code of conduct" is a set of established rules focused both internally and externally on how members act with other organizations. The difference between these two terms, although subtle, is important to note and is the focus of the latter part of this study.

Cyber Expansion, Global Contraction. The cyber environment is growing exponentially.[7] Information and communications systems are directly linked to almost every aspect of our lives today.[8] Both civilian and military organizations operate using millions of computers that control information and communications systems, power grids, nuclear power stations, sewage plants, transportation systems, and healthcare records.[9] In March 2001, there were 458 million Internet users around the globe. By January 2008, the number of Internet users skyrocketed to 1.3 billion. In 1970 there was only one Internet host, but by 2008 this number climbed to 500 million, and by 2015 the number of Internet hosts is expected to exceed the human population of more than 10 billion.[10]

A growing concern for the U.S. military is that nearly 95 percent of its' information flows through the Public Switched Network, and civilian contractors handle a growing portion of the operation and maintenance of military networks. In addition, as the Internet has grown, network providers have begun to funnel Internet traffic by placing large numbers of nodes in consolidated locations to more easily maintain the system, which drastically increases the severity of cyber attacks.[11]

Escalation of Cyber Security Threats. With the rapid increase in usage of information and communications systems over the last twenty years, there has been a corresponding increase in the number of U.S. cyber attacks. With this unprecedented explosion of cyber attacks, it is clear that the U.S. may be facing the most serious economic and national security challenge of the 21st Century, and possibly in its' history.[12] The U.S. is being attacked through its' telecommunications systems at an unparalleled rate, which will require proactive measures to detect and prevent intrusions as they occur.[13] As cyber enemies become more sophisticated in their methods, they severely threaten the United States' information and communications systems. These "hackers" infiltrate into the systems and steal sensitive information from the government and private sectors.[14] Former Vice-Admiral Mike McConnell, head of the National Security Agency from 1992 to 1996, stated that these actions equate to cyber warfare, and the U.S. is currently losing the battle due to severely inadequate cyber-defenses.[15] Although others argue that we are not in a war, it is widely agreed that cyber attacks are occurring and have exposed cyber systems, causing substantial financial losses and costly defensive measures.[16]

Spyware has become the leading form of cyber attack and has increased substantially over the last two decades.[17] Spyware uses web browsers as its' primary means of attack, and is able to penetrate all systems, including government, business, and personal computers.[18] Although many attempts have been made to mitigate the risk of Spyware, including patches, firewalls, and anti-virus software, they have been no match for this unassailable infection.[19] With spyware, it is difficult to know that someone is monitoring your actions on your personal computer. For instance, consider a

hypothetical situation where another nation state uses spyware to hack into the U.S. government financial system and monitors government financial transactions. The U.S. government may be virtually blind to the fact that another nation state is monitoring their transactions, and this lack of oversight could be detrimental to the economic well being of the nation.

Probably the most significant aspect of cyber attacks is that they can be employed from anywhere in the world. Couple this with the speed with which a cyber attack can be executed, and the low cost of employment, and it becomes clear why this type of attack is very attractive to enemies. In addition, it is almost impossible identify an attack before it has occurred, and thus without international cooperation, cyber attacks are difficult to prevent.[20] With the low cost of employment and the ease with which an attack can be carried out, the only real barrier for anyone wanting to conduct cyber attacks is their technological skills.[21]

Cyber Attack Scenarios. With the increasing technological advances in information and communications systems, coupled with an escalation of cyber security threats, the new methods by which cyber warfare can be conducted against the U.S. is daunting. There is no graver threat to our national sovereignty than the endless stream of attacks that have come to fruition with these new technologies.[22] The U.S. is exposed to new threats daily, creating a situation that makes the management of these risks overwhelming. The scenarios listed below are only a few of the many methods cyber attackers can use.

Consider a scenario where the financial records of one of the major banks in the U.S. are hacked into and millions of customer bank accounts are destroyed along with

any evidence of existence.[23] Confusion would arise as the bank struggles to find a solution to fix the situation. If the bank was prepared, it would have a backup system to restore the accounts, but what if the backup was destroyed as well. The bank would have no way of recovering the lost data, and panic would ensue. Within a very short time, millions of U.S. citizens would have no funds to cover living expenses. This type of scenario alone could cause a financial meltdown.

The health care industry today is linked by a massive online collaboration that allows the filing, maintaining, and sharing of health care records at the click of a button. This has revolutionized the industry by providing health care professionals a fast, easy way to access and share patient health records. Now consider a second scenario where a cyber attack is executed against this health care system and thousands of records are damaged or destroyed.[24] Although this scenario may not be as catastrophic as an attack on the financial system, this could be devastating to the health care industry, causing a huge shut down until the issue is contained and eventually resolved.

A third scenario could involve military operations. Consider what would happen if the military of a U.S. adversary developed a cyber weapon that disabled the U.S. infrastructure. This type of cyber weapon could be used for both civilian and military targets depending on the enemy's intent. Past kinetic weapons have been used by nations to destroy enemy infrastructure such as power plants and transport systems, which would disable the system for a lengthy period of time until the system could be rebuilt. However, this new cyber weapon would not need to use kinetic measures to destroy its' target, but could disable the same infrastructure without destroying it. In the example of a power plant, the power grid could be shut off through a cyber attack and

made inoperable for the duration of hostilities, then turned back on when the military operation was completed.[25]

Thousands of airplanes fly over the United States on a daily basis, all monitored and controlled by the Air Traffic Control system. This system monitors air traffic for the entire continental U.S. to ensure that each airplane in the sky has a clear flight from takeoff at its' point of origin to landing at its' destination. A fourth scenario could involve a cyber attack on the Air Traffic Control system that operates on one large, connected system.[26] Such an attack could shut down the Air Traffic Control system, preventing air traffic controllers from monitoring flying aircraft, causing partial blindness in the sky. Although airplane pilots could monitor their airspace using the aircraft navigation system, it would be difficult to see other approaching aircraft and landing would become extremely treacherous.

Another method within the realm of possibility could be an enemy cyber attack on the media.[27] Ponder the idea of what it would be like if an attack was occurring in the U.S. and the media stations were shut down. Limited or no access to information about the attack could cause panic among the American population. In addition to shutting down the media, the enemy could use a media station by replacing the signal with its' own programming and broadcast propaganda. The enemy programming could broadcast false information in many forms, including soldier movements and false destruction of American property and lives. Although actions such as this would not be effective by itself, it could be used effectively as part of a larger operation.[28] However, this type of cyber attack would have it's limitations since there are many broadcast stations in the U.S. and this type of attack would require more centralized media.

U.S. President on Cyber Security

In May 2010, the U.S. President addressed cyber security in the 2010 National Security Strategy, commenting that cyber warfare is one of the most serious security threats that the U.S. has faced as a nation. He stated that the technologies that make us a great nation also empower enemies that want to destroy what the U.S. has accomplished. The President continued by stating that the nation's digital infrastructure is a strategic asset, and the U.S. must make the defense of this asset a priority by ensuring that U.S. networks are secure from cyber attacks.[29] He concludes his comments by stating that the U.S. will deter, prevent, detect, defend, and quickly recover from cyber attacks by investing in people and technology, and strengthening our partnerships both domestically and internationally.[30]

In the 2010 Cyberspace Policy Review, the U.S. President made statements indicating that the U.S. is at a crossroads in terms of securing the nation against cyber attacks. President Obama indicated that current cyber security risks are very serious and must be addressed to ensure economic and national security stability in the 21st century. He stated that there are a growing number of state and non-state actors that are targeting the United States with the ability to compromise and destroy our information systems. He went on to explain that the status quo in cyber security is no longer acceptable, but that the U.S. must address this issue with strong leadership and vision. In doing this, he explains that cyber security roles and responsibilities must be clarified within federal departments and new policies established that empower these departments to execute cyber initiatives.[31] The President concluded by stating that the U.S. approach regarding cyber security over the last 15 years is no longer sufficient, and new cyber security policies and procedures must be established.[32]

The comments made in both the 2010 National Security Strategy and the 2010 Cyberspace Policy Review both indicate that the U.S. President is serious about making cyber security a national security priority. He understands that the current rules of engagement are not sufficient, and realizes that changes must be made to adjust to the increase in frequency and sophistication of cyber attacks. To adjust to the increase in cyber security threats, the U.S. President established guidelines for the defense chain of command so that new rules of engagement could be established. See Figure 1 for the specific guidelines provided by the U.S. President regarding cyber security as presented in the 2010 National Security Strategy and 2010 Cyberspace Policy Review. There appears to be sufficient emphasis on cyber security from the leader of the nation, so the focus of the next section shifts down the chain of command to the DoD to see if this emphasis continues.

U.S. PRESIDENT GUIDELINES FOR CYBER SECURITY
Sharing Responsibility for Cyber Security. The Federal government cannot succeed in the many facets of securing cyberspace if it works in isolation. The public and private sectors' interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government services depend. Government and industry leaders—both nationally and internationally—need to delineate roles and responsibilities, integrate capabilities, and take ownership of the problem to develop holistic solutions. Only through such partnerships will the United States be able to enhance cyber security and reap the full benefits of the digital revolution. The global challenge of securing cyberspace requires an increased effort in multilateral forums. This effort should seek—in continued collaboration with the private sector—to improve the security of interoperable networks through the development of global standards, expand the legal system's capacity to combat cyber crime, continue to develop and promote best practices, and maintain stable and effective Internet governance.
Partner Effectively With the International Community. International norms are critical to establishing a secure and thriving digital infrastructure. The United States needs to develop a strategy designed to shape the international environment and bring like-minded nations together on a host of issues, including acceptable norms regarding territorial jurisdiction, sovereign responsibility, and use of force. In addition, differing national and regional laws and practices—such as those laws concerning the investigation and prosecution of cyber crime; data preservation, protection and privacy; and approaches for network defense and response to cyber attacks—present serious challenges to achieving a safe, secure, and resilient digital environment. Addressing these issues requires the United States to work with all countries— including those in the developing world who face these issues as they build their digital economies and infrastructures—plus international bodies, military allies, and intelligence partners.

Figure 1. U.S. President Cyber Security Guidelines[33]

U.S. Department of Defense on Cyber Security

One of the primary responsibilities assigned to the DoD is to protect and defend the U.S. population. Since cyber has become the latest means of attack against the U.S., it is incumbent upon the DoD to analyze this new threat and adjust its' rules of engagement accordingly. Whether the DoD has planned and adjusted appropriately to this new threat is the main argument of this section. First, an overview of the DoD's role in cyber security is provided, followed by a description of the legal authorizations that enable the U.S. to execute national defense, particularly against cyber attacks. Next, the U.S. Secretary of Defense's (SecDef) perspective on cyber security is analyzed through his comments in the 2010 Quadrennial Defense Review, followed by an analysis of the Joint Chiefs of Staff (JCofS) perspective as identified in the 2006 National Military Strategy for Cyberspace Operations. This section concludes with an overview of the establishment of the U.S. Cyber Command, and a discussion on how this information ties into the sufficiency of the U.S. in protecting its' information and communications systems against cyber attacks.

Department of Defense Role in Cyber Security. U.S. legal statutes and national policy state that the DoD is assigned three primary roles, including the defense of the nation, national incident response, and critical infrastructure protection. The DoD is the only agency within the U.S. that is authorized to conduct military operations in support of its' primary roles. Within the cyber realm, the DoD must defend the nation by executing military operations to defeat, dissuade, and deter cyber attacks, including the exploitation of enemy networks to gather intelligence necessary to plan and execute both offensive and defensive operations. The DoD is also charged with providing military support to civil authorities in response to cyber threats.[34] Finally, the DoD must

provide cyber infrastructure protection to ensure the nation's cyber networks remain available to support the full range of military operations.[35]

Legal Authorities for Cyber Security. The U.S. Armed Forces have authority to take military actions as assigned by the U.S. Constitution and Federal law. The authority derived from these legal documents provides the roles and responsibilities for military organizations to develop the necessary capabilities and expertise required for specific operations. Included in these documents are authorities for conducting cyber operations. Figure 2 identifies the key legal authorities that apply to the DoD in conducting cyber operations, including Title 10, Armed Forces; Title 32, National Guard; and Title 50, War and National Defense.[36]

US Code	Title	Key Focus	Principal Organization	Role in Cyberspace
Title 6	Domestic Security	Homeland Security	Department of Homeland Security	Security of US Cyberspace
Title 10	Armed Forces	National Defense	Department of Defense	Secure US Interests by Conducting Military Operations in Cyberspace
Title 18	Crimes and Criminal Procedure	Law Enforcement	Department of Justice	Crime Prevention, Apprehension, and Prosecution of Cyberspace Criminals
Title 32	National Guard	First Line Defense of the United States	Army National Guard, Air National Guard	Support Defense of US Interests in Cyberspace through Critical Infrastructure Protection, Domestic Consequence Management, and Other Homeland Defense-Related Activities
Title 40	Public Buildings, Property, and Works	Chief Information Officer Roles and Responsibilities	All Federal Departments and Agencies	Establish and Enforce Standards for Acquisition and Security of Information Technologies
Title 50	War and National Defense	Foreign Intelligence and Counter-intelligence Activities	Intelligence Community Agencies Aligned under the Office of the DNI	Intelligence Gathering through Cyberspace on Foreign Intentions, Operations, and Capabilities

Figure 2. Legal Authorities[37]

Secretary of Defense on Cyber Security. The SecDef made statements in the 2010 Quadrennial Defense Review that DoD assessments regarding conflicts against enemy nation states indicated that current U.S. rules of engagement are not sufficient to

counter cyber attacks. He stated that cyberspace has become a domain just as significant as those of land, sea, air, and space, and DoD has become very dependent on this domain for military command and control, intelligence, logistics, and weapons technologies. The SecDef went so far as to say that the military cannot conduct effective operations without the information and communications systems that cyberspace provides.[38]

The SecDef also noted that enemy nation states are now targeting the U.S. information and communications systems to interrupt or prevent U.S. military operations because they know that the DoD has become so reliant on these systems. He stated that the DoD must defend the U.S against these cyber attacks, but that it is a very difficult task given the number of computer networks, military installations, and computers in use around the world every day. Couple this with the increase in frequency and speed of cyber attacks and the anonymity of cyberspace, and cyber defense becomes even more overwhelming.[39]

As directed by the U.S. President in the 2010 National Security Strategy, the SecDef made cyber security a priority in his statements in the February 2010 Quadrennial Defense Review. The SecDef addressed the U.S. President's directives, and took further steps by identifying cyberspace as a separate domain, and identifying steps for the DoD to take that will aid in deterring enemy states from conducting cyber attacks against the U.S., particularly the establishment of the U.S. Cyber Command (USCYBERCOM). See Figure 3 for the specific guidelines provided by the SecDef regarding cyber security as presented in the 2010 Quadrennial Defense Review. All

indications show that the DoD is taking the necessary steps to protect the U.S. against cyber attacks.

SECDEF GUIDELINES FOR CYBER SECURITY
Develop a comprehensive approach to DoD operations in cyberspace. A Department-wide comprehensive approach will help build an environment in which cyber security and the ability to operate effectively in cyberspace are viewed as priorities for DoD. Strategies and policies to improve cyber defense in depth, resiliency of networks, and surety of data and communication will allow DoD to continue to have confidence in its cyberspace operations. A central component of this approach is cultural and organizational: The Department will adapt and improve operational planning, its networks, its organizational structures, and its relationships with interagency, industry, and international partners.
Develop greater cyberspace expertise and awareness. The Department will redouble its efforts to imbue its personnel with a greater appreciation for the threats and vulnerabilities in the cyber domain and to give them the skills to counter those threats and reduce those vulnerabilities at the user and system administrator levels. DoD can no longer afford to have users think of its information technologies and networks as simply the benign infrastructure that facilitates their work. Users and managers must be held accountable for ensuring network security and for implementing best practices. DoD is also growing its cadre of cyber experts to protect and defend its information networks and is investing in and developing the latest technologies.
Centralize command of cyberspace operations. In an effort to organize and standardize cyber practices and operations more effectively, the DoD is standing up U.S. Cyber Command (USCYBERCOM), a sub-unified command under U.S. Strategic Command, to lead, integrate and better coordinate the day-to-day defense, protection, and operation of DoD networks. USCYBERCOM will direct the operation and defense of DoD's information networks, and will prepare to, and when directed, conduct full spectrum cyberspace military operations. An operational USCYBERCOM will also play a leading role in helping to integrate cyber operations into operational and contingency planning.
Enhance partnerships with other agencies and governments. Freedom of operation in cyberspace is important and DoD must have the capabilities to defend its own networks. However, the interdependence of cyberspace means DoD networks are heavily dependent on commercial infrastructure. Just as it does in conducting many of our missions, DoD needs to collaborate with other U.S. departments and agencies and international partners both to support their efforts and to ensure our ability to operate in cyberspace. This mutual assistance includes information sharing, support for law enforcement, defense support to civil authorities, and homeland defense.

Figure 3. U.S. SecDef Cyber Security Guidelines[40]

Joint Chiefs of Staff on Cyber Security. From a joint perspective, the JCofS produced the 2006 National Military Strategy for Cyberspace Operations. The JCofS state that the U.S. is no longer operating as a separate entity, but that it is intertwined in a global network of interdependence that is plagued by uncertainty, complexity, and continual change. The U.S. has its' critical infrastructure integrated into this cyber network, including government departments, businesses, health care organizations, and national security agencies. The JCofS produced the National Military Strategy for

Cyberspace Operations as the vehicle to ensure the U.S. maintains superiority in cyberspace.[41]

The JCofS also identify cyberspace as a domain, and state that, like the other domains, it has associated risks. In analyzing the risks, there are certain considerations that the JCofS provide. The first is that the U.S. military reliance on cyberspace will continue to increase over time, which provides the enemy with a means of taking advantage of this dependence. Another risk is that a lack of properly trained and equipped personnel may increase the already vulnerable cyber networks. Common standard operating procedures must be incorporated into training to alleviate this risk. Finally, without persistent efforts to stay ahead of adversaries, the U.S. will lose the advantage it has in cyberspace.[42]

The JCofS produced the 2006 National Military Strategy for Cyberspace Operations, in which they state that the only way the U.S. can continue to have freedom of action is to deny the enemy cyberspace superiority. They continued that the DoD must provide new military options to ensure the U.S. maintains its' cyberspace superiority. The 2006 National Military Strategy for Cyberspace Operations is the JCofS's attempt to provide a new military option to the current rules of engagement, indicating that the JCofS are committed to updating current U.S. policy to counter the growing cyber threat.

This section analyzed the perspectives of some of the top U.S. government defense officials to determine their views on the current cyber security rules of engagement. After reviewing documents prepared by the U.S. President, the SecDef, and the JCofS, there is unanimity among the top government officials in terms of the

proper methods in defending the U.S. against cyber attacks. All were in agreement that the current U.S. cyber security rules of engagement are not sufficient to protect the U.S. information and communications systems against cyber attacks. The directives established by the U.S. President regarding the necessary changes in cyber security were properly received by the SecDef and the JCofS, and were subsequently incorporated into their defense plans. With the establishment of the USCYBERCOM, the discussion focuses on whether this joint command is equipped to execute this extremely critical task, and whether they properly disseminated these directives down to the U.S. Army, Navy, and Air Force to ensure they are incorporated into doctrine at the lowest levels of defense. This issue is examined in the next several sections of this study.

U.S. Cyber Command on Cyber Security

Probably the most significant step the DoD took to address the growing cyber security threat was the directive to establish USCYBERCOM, which was established to strengthen the DoD capabilities in cyberspace and to provide a centralized command that conducts cyber operations. USCYBERCOM is charged to lead, integrate, and coordinate the daily defense, protection, and operation of all DoD networks. It is also charged, when directed, to conduct full spectrum cyberspace military operations.[43]

The designated Commander, Army General Keith B. Alexander, was assigned to establish this command and carry out the responsibilities as directed by the U.S. President and Congress.[44] General Alexander concedes that the current rules of engagement are not sufficient to protect the U.S. information and communications systems from cyber attacks. He argues that the current rules are not adequate because

they were not designed to incorporate the many diverse parties that make up cyberspace today. The only way to produce rules of engagement that are effective across the broad spectrum of cyberspace is to ensure that all domestic and international parties involved understand and abide by a cooperative agreement that establishes a standardized code of conduct. USCYBERCOM has a daunting task in this respect as it requires the integration of information technology offices from multiple organizations, including the military services, all combatant commands, all offices in the national intelligence community, several private sector agencies, and nation states that have a role in cyberspace technologies.[45]

In a recent interview, General Alexander clarified the difficulty of the USCYBERCOM mission by providing an example of a cyber attack.[46] In this example, he explains that every adversarial state has different standing rules of engagement for cyber security, and the only way for the U.S. to gain success in this environment is to produce a consolidated set of rules, or code of conduct.[47] In a more recent article, it was made clear that the USCYBERCOM is finding this task more difficult than originally anticipated, and that attempts to establish a new code of conduct are falling far behind.[48] What amplifies the slow progress in generating this code of conduct is the increase in global funding of cyber warfare and the sophistication with which cyber weapons are produced.[49] A recent example of improved cyber weaponry is the Stuxnet worm that disabled Iran's nuclear program by spreading through flaws in Microsoft Windows.[50]

USCYBERCOM will continue to address the issue of finding common ground in establishing a code of conduct for cyberspace, but until it finds a way to speed up

production on this critical issue, progress will be extremely slow. The resulting impact on the Army, Navy and Air Force is they are utilizing rules of engagement that are not designed to handle the current modern and more sophisticated cyber threats that continue to escalate. The next several sections examine what the military services are doing in the interim until this new standardized code of conduct is established.

U.S. Military Services on Cyber Security

Based on the guidelines provided by the U.S. President and SecDef, and in light of the deficiencies in cyber security policies, the military services have begun the transition toward incorporating a more robust cyber security program into their operations. There are several initiatives each military service is undertaking to prepare for the necessary changes in cyber security. This section addresses the current cyber security standing rules of engagement for the military services representing the Air (U.S. Air Force), Land (U.S. Army), and Sea (U.S. Navy) domains. These initiatives have been implemented to make the transition to a new code of conduct that will provide the required protection of our information and communications systems.

Air Force on Cyber Security. The Air Force seems to be leading the way in terms of adjusting its cyber security rules of engagement. The Air Force was aware early on that the rules they had established for the protection of these critical systems were not sufficient, so as early as 2007 they began reviewing their policies and procedures in an attempt to improve their rules of engagement to meet the new cyber security threats. The previous Air Force rules concentrated inward on information security, information protection, and information operations, but were not focused on the broader scope of cyber security because prior to the last decade cyber warfare was not a substantial

threat. By July 2010, the Air Force established new rules that focused on cyber security as a whole within the cyberspace domain. It did this by establishing new cyberspace fundamentals and a new design, planning, execution, and assessment program.[51]

As described by the Air Force, cyberspace fundamentals include cyberspace operations, which are defined as: "The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid."[52] Air Force cyberspace fundamentals also explain cyberspace as a man-made domain, unlike the other domains, which requires continued human attention.[53] Also discussed are the military challenges that are inherent in cyberspace,[54] and the importance of integrating cyberspace operations across all domains.[55] With the creation of cyberspace operations, the Air Force needed to create a new design, planning, execution, and assessment program specific for the new cyberspace domain.[56] The cyberspace design has to incorporate the capability to react quickly because of the short reaction time between execution and effect of a cyber attack.[57] The U.S. no longer has the luxury of a twenty-minute window from launch to effect of an attack.[58] For instance, a cyber attack designed to disable the U.S. electrical power grid could be initiated from an unknown site, shutting down the power within seconds of launch.[59] Planning should focus on the advantages of cyberspace operations, the dangers of unintended consequences, and close coordination between all organizations involved in cyberspace operations.[60] Execution of cyberspace operations requires the integration of cyberspace effects into a time-phased scheme of maneuver and fires, and

an assessment in cyberspace involves evaluating effects following the same procedures as any other Air Force operation.[61]

The Air Force was a year ahead of the other services when it activated Air Force Cyber Command (AFCYBER) in the fall of 2009.[62] The current Commander of AFCYBER, Major General Richard E. Webber, in his testimony before the House Armed Services Committee on September 23, 2010, provided several initiatives the Air Force is undertaking to improve its role in providing security to vital U.S. information and communications systems.[63] Webber explained that military reliance on cyber has increased exponentially over the last several decades to the point where successful military operations have become dependent on cyberspace.[64] This dependence requires the military to establish a standardized process that is focused on achieving objectives using cyberspace as a critical tool.[65] The AFCYBER mission is to "plan and conduct cyberspace operations in support of the combatant commands and to maintain and defend the Air Force Enterprise Network."[66]

In addition to the activation of AFCYBER, the Air Force has implemented several initiatives in support of USCYBERCOM. First, they began extensive internal collaboration to integrate cyberspace rules of engagement into operational plans, which transformed cyber from performing a support role of protecting the network to a primary role of protecting the mission. Second, the Air Force sought and obtained dedicated intelligence resources in support of cyber operations, which shifted cyber operations from a reactive defense mode to a proactive mode of predicting and preventing cyber attacks. Third, the Air Force restructured its cyber workforce and refocused cyber training toward producing personnel with an operational mindset that is focused on

protecting the mission. Finally, the Air Force sought to provide cyber personnel with the tools they needed to operate successfully and in a timely manner, and thus they streamlined their acquisition process.[67]

Army on Cyber Security. The current Army rules of engagement for protecting critical information and communications systems primarily focus on the Army infrastructure. This internal focus provides Army personnel with a set of rules to ensure Army systems remain secure. The Army identifies these procedures using several security categories, information security for the classification of information, and information systems security for the protection of information used on automated systems.

Army information security relates to the protection of classified information that is deemed, in the interest of national security, to require protection against disclosure to unauthorized personnel. It specifically establishes requirements to ensure information is protected through proper handling, including the classifying, downgrading, declassifying, transmitting, transporting, and safeguarding of information.[68] The rules established apply to all Army personnel, and charge them with the responsibility of properly safeguarding and protecting any information to which they have access, particularly classified information. Army personnel are provided three categories for classifying information in order to assist them in their efforts: top secret, secret, and confidential. It is incumbent upon all Army personnel to properly classify information using one of these categories, and to use due diligence to ensure that information is adequately protected from compromise.[69] The rules that Army personnel must follow in

handling information are discussed in minute detail to ensure the protection of Army information from leakage to unauthorized personnel.

Army information systems security describes the rules of engagement established to protect classified or sensitive information that is processed, stored, or transmitted over automated information systems. There are two subcategories of information systems security: computer security and communications security. Computer security provides safeguards to protect classified or sensitive information used in any form on a computer system.[70] There are many rules established to ensure the proper protections on computer systems, some of which include accountability of personnel for their actions on a computer, access control to only allow access to authorized personnel, security and awareness training for all personnel accessing a computer, and control measures that prevent unauthorized disclosure, destruction, or modification of automated systems.[71]

Army communications security establishes rules that are designed to deny unauthorized personnel from gaining access to classified or sensitive information while it is being electronically transmitted from sender to receiver.[72] An entire regulation was established that provides the vast rules that protect the Army against unauthorized access, but a few general rules include: only allow approved cryptographic systems within the Army; equipment with commercially developed algorithms cannot be used for classified information; equipment users must understand that their use of an Army system constitutes consent to monitoring.[73] Still another regulation provides rules that establish the monitoring of information systems and guidance for the monitoring of

information systems by Army organizations tasked with conducting monitoring operations.[74]

There are several initiatives the Army established to protect against potential cyber threats. The Army is working with USCYBERCOM to establish new rules of engagement with the domestic and international communities. They are doing this primarily by establishing their own cyber command called Army Forces Cyber Command (ARFORCYBER). This command was established in October 2010 in support of USCYBERCOM with the mission to "plan, coordinate, integrate, synchronize, direct, and conduct network operations in defense of all Army networks and mission objectives."[75] The Commander of ARFORCYBER, Major General Hernandez, argues that ARFORCYBER's success lies within its' joint capability to operate along side many participants, including internal organizations such as the Army components and Combatant Commanders, but also with domestic and international partners like other U.S. military services, national agencies, private sector organizations, and nation states within the international community.[76] The ARFORCYBER Commander grasps the magnitude of future challenges, including the speed with which cyber threats can be employed, the unclear nature of cyberspace boundaries, and the potential for simultaneous cyber attacks in multiple locations.[77]

ARFORCYBER is also undertaking several initiatives to make certain they are prepared for potential cyber security threats. Since training is a key component in the defense against cyber attacks, ARFORCYBER is investing heavily in educating and training Army personnel to understand the new threats and be able to develop and employ new capabilities.[78] ARFORCYBER is also investing in technically proficient

people to posture itself for success in combating cyber threats by establishing a total strength of 21,000 personnel for the ARFORCYBER headquarters out of Fort Belvoir, Virginia.[79] ARFORCYBER argues that it must have network visibility, and thus is investing in technology to transform the Army network system into a single network that standardizes security capability and provides the visibility necessary for the Army to protect its vital systems.[80] Finally, ARFORCYBER is coordinating with U.S. Army Training and Doctrine Command to incorporate cyber operations into a doctrinal plan that the Army will use to conduct cyber operations from 2016-2028.[81]

Navy on Cyber Security. The current rules of engagement used by the Navy are similar to the Army rules in many respects; they also focus on protecting their information and communications infrastructure. The Navy established standardized practices designed to aid its service members in securing its telecommunication systems against cyber attacks. The Navy identifies its rules of engagement using three categories nearly identical to the Army rules, including information security, information systems security, and communications security. The slight differences between the Navy and Army rules include the subcategory of information security called information assurance, and several subcategories of communications security. The current Navy rules of engagement on cyber security are discussed below.

Navy information security is described as the rules established to protect from unauthorized disclosure of information that may be deemed to cause damage to U.S. national security.[82] Navy information assurance is defined as the measures the Department of Navy takes to ensure information is protected from unauthorized disclosure, including the protection and availability of information systems.[83] The Navy

information security program is designed to establish standardized rules of engagement for the classification, safeguarding, transmission and destruction of classified information.[84] Like the other military services, the Navy uses three levels of classification: top secret, secret, and confidential. The rules to which Navy personnel must abide are provided in great detail in Navy security manuals, and will not be discussed in such depth in this study. However, some of the rules include: all information assurance personnel must be properly trained and certified;[85] Navy personnel must be DoD trained prior to access to any Navy information systems;[86] and Navy Commanders must control remote access to Navy information systems and networks.[87]

Navy information systems security is designed to provide rules for Navy personnel to follow that ensure information systems are secure from unauthorized disclosure of information that is collected, processed, transmitted, stored, or disseminated within these systems.[88] Once again, the rules of engagement are much too lengthy to discuss in this study, but some of the rules are provided to give an idea of the Navy's perspective on information systems security. Some of the information systems security rules established by the Navy include limitations on Local Area Network access, passwords, electronic mail, Internet web browsing, and games.[89] In terms of Local Area Networks, the Navy requires all users to submit a request to be approved for access.[90] There are many stipulations on what can be used as a password to access an information system, including no use of dictionary words, and no user names or birth dates.[91] Electronic mail can only be used for official business, and will be monitored for unauthorized events such as hacking or virus attacks.[92] Internet

web browsing is also for official business only, and will be monitored for any unauthorized use such as accessing information related to pornography, racism, bigotry or anti-semitism.[93] All games are prohibited from use on any Navy information systems.[94] These are only a few of the many established rules of engagement relating to Navy information systems security.

Navy communications security is described as the measures taken to ensure information related to U.S. national security that is derived from information systems is protected from unauthorized disclosure. There are several subcategories of communications security, which include crypto security, physical security, transmission security, and emission security. Crypto security is a type of communications security that provides technically sound cryptosystems. Physical security involves the physical measures that are taken to protect communications material. Transmission security relates to measures taken to safeguard transmissions from the possibility of interception or exploitation, and emission security involves actions designed to deny unauthorized access to classified information retrieved from the interception of emanations.[95] The Navy has well-established rules for protecting communication systems that will not be discussed in this study.

The Navy activated its Fleet Cyber Command (FLCYBERCOM) in January 2010 with its first Commander, Vice Admiral Bernard J. McCullough, III. FLCYBERCOM is one of many initiatives the Navy has implemented to counter the new cyberspace domain and the challenges involved in protecting the Navy information and communications systems against more sophisticated cyber attacks. The FLCYBERCOM mission is to direct Navy cyberspace operations in order to deter and

defeat cyber security threats that attempt to prevent freedom of action in cyberspace. This command has consolidated Navy efforts into one central authority that directs many Navy operations sectors including networking, cryptology, signals intelligence, information operations, cyber, electronic warfare and space.[96] This central authority will allow the Navy to respond quickly to cyber threats on their networks and maintain its critical information assurance capability.[97]

Critical to the success of FLCYBERCOM are some initiatives the Navy has implemented to shape its role in the protection of vital U.S. information and communications systems. These initiatives include creating an appropriate FLCYBERCOM structure, developing personnel cyber skills through recruitment and training, developing partnerships with the private sector, and coordinating efforts across domains, all in an effort to combat cyber attacks.[98] To structure FLCYBERCOM, the Navy has constructed a Navy task force that assigns regional responsibilities to subordinate groups. These task groups have specific responsibilities, including Navy network operations, information operations, and research and development designed to develop new technologies to counter cyber threats.[99] To stay ahead of the new advanced cyber threats, the Navy is developing a new training program designed to produce personnel who are technologically proficient and can apply these skills to combat cyber attacks.[100] The Navy is also partnering with industry, academia, and research and development centers to incorporate private sector expertise that will provide the Navy with the required knowledge and capabilities to counter cyber threats.[101] Finally, the Navy understands that they must coordinate across all domains to provide the necessary security of all interconnected systems.[102]

This section introduced the military service's perspective on whether the current rules of engagement are sufficient to protect the U.S. information and communications systems against cyber attacks. The Leaders of the Army and Navy are aware that their current cyber rules are insufficient, and they have taken steps, as directed by the SecDef, to prepare for the new challenges inherent in modern cyberspace. The Air Force is ahead of the other military services in that it stood up its cyber command well in advance of the other services and has already established new rules of engagement. After reviewing the rules established in several military service manuals, it is clear that these procedures were focused inward with no regard for the many organizations that play a role in cyberspace both domestically and internationally.

Generating a Global Cyber Code of Conduct

This study argued that the military services, who are charged with the protection of U.S. national security interests in the air, land, sea, and now cyberspace domains, have current rules of engagement that are not sufficient to protect U.S. information and communications systems against cyber attacks. Directives have been passed down the defense chain of command from the U.S. President, through the SecDef, to the military services to transform their current rules to new policies providing the required protection against faster, more frequent, and more sophisticated cyberspace threats. Beginning in 2009, the military services embarked on a plan to address these cyberspace challenges, creating new commands like USCYBERCOM, ARFORCYBER, FLCYBERCOM, and AFCYBER, in order to provide critically needed protection. But there are several indications that these actions are not enough.

The military services' actions to activate cyber commands, in an effort to protect U.S. information and communications systems, are the right steps toward creating the infrastructure required to combat cyber threats. However, these actions are only a starting point given the growing nature of the threat. Growing cyberspace threats indicate that much more is needed to protect U.S. systems against these attacks. The increasing sophistication of cyber attacks is making it ever more difficult to protect vital U.S. systems.[103] A great example of this sophistication is an attack in 2010 where the Stuxnet computer worm used previously unknown flaws in Microsoft Windows software to disable centrifuges in Iran's nuclear program.[104] Another concern with cyber attacks is the anonymity with which attacks can be conducted. A cyber attack can be filtered through many systems that are taken over by a hacker in order to mask the original launch location of the attack. This new technology makes it very difficult to trace the originator of an attack, which raises the problem of attribution.[105]

Other concerns are the speed and frequency with which cyber attacks can be executed. Cyber attacks are becoming increasingly faster and can occur in a millisecond without warning, so preventing these attacks is becoming extremely difficult.[106] In addition, U.S. information and communications systems are bombarded with millions of cyber attacks daily, so the shear frequency of these attacks makes it difficult to provide the necessary protection.[107]

The government reaction time involving the establishment of such a plan appears to be lagging far behind the threat capability. With this latency in reacting to the threat, the military services appear to remain in a reactionary mode until they can implement their plans. Although the Air Force seems to be further ahead in planning, most

services' current rules of engagement tend to focus inward on the behavior of individuals within the organization, while cyber attacks are an international problem requiring behavioral changes on a global scale. Current cyber threats require cooperation not only domestically, but internationally as well. Since cyberspace is a global domain, protecting against cyber threats requires global solutions.

From a nation state perspective, the solution lies in creating global cooperation, or agreement, that establishes rules of the road on an international scale. Because the definition of the term "rules of engagement" from a military perspective tends to focus inward on the actions of individuals, the term "code of conduct" emphasizes a broader, all-encompassing view, and therefore seems more appropriate in addressing a global agreement. As described by Hamadoun Toure, a secretary-general of the United Nations-affiliated International Telecommunications Union, new technology has bridged the gap between cyberspace and the real world, and it is critical to establish a global code of conduct that bans unacceptable actions such as disabling networks and data theft.[108] This code of conduct would establish rules banning aggressive cyber attacks and place the responsibility of investigating and correcting violations on the nation state where an attack originated.[109]

Establishing a global cyber code of conduct provides rules that ban negative behavior in cyberspace, place responsibility to nation states where this behavior originates, and establish consequences on the perpetrators of these negative actions. This code of conduct would help the U.S. military services' efforts to protect U.S. information and communications systems against cyber attacks through global rules that prevent specific cyber behavior. By utilizing rules of engagement internally to

modify individual behavior and a code of conduct to help modify external behavior within the global community, the U.S. reveals a more comprehensive approach to solving cyber related threats.

Conclusion

Understanding whether the current cyber rules of engagement are sufficient to protect U.S. information and communications systems is critical in determining future efforts toward mitigating cyber attacks not only against the U.S., but also on a global scale. This study argues that the current U.S. cyber rules of engagement are not sufficient, and that in order to counter the growing increase in speed, frequency, and sophistication of cyber attacks, a new strategy must be implemented quickly to create new capabilities before cyber threats become unmanageable. Given the global nature of cyber attacks, there must likewise be a global solution in the form of a code of conduct that establishes international cooperation through a set of rules that ban negative or destructive behavior in cyberspace. Placing responsibility on nation states where behavior originates and providing consequences as appropriate is one goal of this code of conduct.

The establishment of a code of conduct is an important starting point for mitigating cyber security threats, but there are many aspects of cyberspace that cannot be fully addressed by this approach. For instance, enforcing a code of conduct may not fully address the issues of anonymity and the lack of time to react to a cyber attack. Further, not all nation states may join the coalition, and there are threats other than nation states, which suggests that a code of conduct is not the only solution. Further

research must be done on ways to mitigate cyber security threats in terms of these other means of cyber attack.

Because of the government delay between formulating a comprehensive cyber security plan and the growing threats in cyberspace, it is critical for the U.S. to plan and implement a code of conduct. It is not enough to wait until the U.S. has a catastrophic event such as a meltdown of the U.S. financial system or critical infrastructure before taking action. The current rules of engagement are totally insufficient to sustain U.S. information and communications systems given the growing cyber threat, and without proper action, eventually one of the cyber attack scenarios discussed in this study will occur.

Endnotes

[1] Jeffrey Kelsey, “Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare,” *Michigan Law Review* 106 (May 2008): 1428.

[2] Stephen Korns and Joshua E. Kastenberg, “Georgia’s Cyber Left Hook,” *Parameters* 38 (Winter 2008-09): 60.

[3] Ibid., 70.

[4] Ollie Washington, *The Legal and Ethical Implications of Information Operations,* Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, April 10, 2001), 1.

[5] *The Oxford Essential Dictionary of the U.S. Military* (New York, NY: Berkley Books, 2001), http://www.oxfordreference.com.ezproxy.library.tufts.edu/views/ENTRY.html?subview=Main&entry=t63.e6938 (accessed January 13, 2011).

[6] Kay Miranda, “Definition of Code of Conduct,” http://www.ehow.com/about_5044074_definition-code-conduct.html#ixzz1AwsrUmtS (accessed January 13, 2011).

[7] Kelsey, Hacking Into International Humanitarian Law,” 1431.

[8] Ibid.

[9] Ibid., 1432.

[10] Steven Smith, “Defending the Nation Against Cyber Attack,” lecture, The Fletcher School of Law and Diplomacy, International Security Studies Program Luncheon, Medford, MA, October 18, 2010, cited with permission of Steven Smith, 5-7.

[11] Kelsey, Hacking Into International Humanitarian Law,” 1432.

[12] Smith, “Defending the Nation,” 3.

[13] Ibid.

[14] National Research Council of the National Academies, *Proceedings of a Workshop On Deterring Cyberattacks: Informing Strategies and Developing Options For U.S. Policy* (Washington, DC: The National Academies Press, 2010), 180.

[15] Ibid., 181.

[16] Ibid.

[17] Mark Barwinski, Cynthia E. Irvine and Tim E. Levin, “Empirical Study of Drive-by-Download Spyware” (University of Maryland Eastern Shore: International Conference on Information Warfare and Security, Princess Anne, MD, March 15, 2006), 1.

[18] Ibid.

[19] Ibid., 10.

[20] Michael Vatis, “The Next Battlefield: The Reality of Virtual Threats,” *Harvard International Review* 28, no. 3 (Fall 2006): 59.

[21] Ibid., 60.

[22] Smith, “Defending the Nation,” 4.

[23] Ibid.

[24] Ibid.

[25] Kelsey, Hacking Into International Humanitarian Law,” 1435.

[26] Smith, “Defending the Nation,” 4.

[27] Kelsey, Hacking Into International Humanitarian Law,” 1435.

[28] Ibid., 1436.

[29] Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 27.

[30] Ibid., 28.

[31] National Security Council, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” The White House, http://www.whitehouse.gov/CyberReview (accessed November 8, 2010), iii.

[32] Ibid., v.

[33] Ibid., 17-20.

[34] Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations* (Washington, DC: U.S. Joint Chiefs of Staff, November 2006), 1.

[35] Ibid., 2.

[36] Ibid., 1.

[37] Ibid., A-1.

[38] Robert M. Gates, *Quadrennial Defense Review Report* (Washington, DC: U.S. Department of Defense, February 2010), 37.

[39] Ibid.

[40] Ibid., 38-9.

[41] Chairman, *The National Military Strategy,* 1.

[42] Ibid., 9.

[43] Gates, *Quadrennial Defense Review,* 38.

[44] Chairman, *The National Military Strategy,* 1.

[45] Ibid.

[46] Ibid., 2.

[47] Ibid.

[48] Joseph Menn, "Rules of Engagement for Cyberwars See Slow Progress," *Financial Times,* December 29, 2010, http://www.proquest.com.ezproxy.library.tufts.edu (accessed January 13, 2011), 4.

[49] Ibid.

[50] Ibid.

[51] U.S. Air Force, *Cyberspace Operations,* Air Force Doctrine Document 3-12 (Washington, DC: Secretary of the Air Force, July 15, 2010), vi.

[52] Ibid., 1.

[53] Ibid., 2.

[54] Ibid., 7.

[55] Ibid., 19.

[56] Ibid., 30.

[57] Ibid.

[58] Vatis, “The Next Battlefield,” 3.

[59] Ibid.

[60] Ibid., 31.

[61] Ibid., 31-2.

[62] Richard E. Webber, “Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations, U.S. Air Force Cyber Command,” *Congressional Record* (September 23, 2010): 2.

[63] Ibid.

[64] Ibid., 1.

[65] Ibid.

[66] Ibid., 2.

[67] Ibid., 3.

[68] U.S. Department of the Army, *Information Security Program,* Army Regulation 380-5 (Washington, DC: U.S. Department of the Army, September 29, 2000), 1.

[69] Ibid., 4.

[70] U.S. Department of the Army, *Information Systems Security,* Army Regulation 380-19 (Washington, DC: U.S. Department of the Army, February 27, 1998), 1.

[71] Ibid., 7.

[72] Ibid., 19.

[73] Ibid.

[74] U.S. Department of the Army, *Information Security Program,* 1.

[75] Rhett Hernandez, "Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations, U.S. Army Forces Cyber Command," *Congressional Record* (September 23, 2010): 2.

[76] Ibid., 4.

[77] Ibid., 7-8.

[78] Ibid., 8.

[79] Ibid., 9.

[80] Ibid.

[81] Ibid., 11.

[82] U.S. Department of the Navy, *Information Security Program,* Secretary of the Navy M-5510.36 (Washington, DC: Chief of Naval Operations, June 30, 2006), A-10.

[83] Ibid.

[84] Ibid., 1.1.

[85] Ibid., 7.

[86] Ibid.

[87] Ibid., 9.

[88] U.S. Department of the Navy, *Information Systems Security Program,* Bureau of Naval Personnel Instruction 5239.1B (Millington, TN: Chief of Naval Personnel, April 5, 2001), 2.

[89] Ibid., 1-4.

[90] Ibid., 1.

[91] Ibid.

[92] ibid.

[93] Ibid., 3.

[94] Ibid., 4.

[95] U.S. Department of the Navy, *Information Security Program,* A-10.

[96] Bernard J. McCullough III, “Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations, U.S. Fleet Cyber Command,” *Congressional Record* (September 23, 2010): 1.

[97] Ibid., 2.

[98] Ibid., 2-5.

[99] Ibid., 3.

[100] Ibid., 4.

[101] Ibid., 4-5.

[102] Ibid.

[103] Vatis, “The Next Battlefield,” 62.

[104] Menn, "Rules of engagement,” 4.

[105] Vatis, “The Next Battlefield,” 62.

[106] Ibid.

[107] Smith, “Defending the Nation,” 9.

[108] Menn, "Rules of engagement,” 4.

[109] Ibid.

BIBLIOGRAPHY

Barwinski, Mark, Cynthia E. Irvine, and Tim E. Levin. “Empirical Study of Drive-by-Download Spyware.” University of Maryland Eastern Shore: International Conference on Information Warfare and Security, Princess Anne, MD, March 15, 2006.

Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations.* Washington, DC: U.S. Joint Chiefs of Staff, November 2006.

Gates, Robert M. *Quadrennial Defense Review Report*. Washington, DC: U.S. Department of Defense, February 2010.

Hernandez, Rhett. “Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations, U.S. Army Forces Cyber Command.” *Congressional Record* (September 23, 2010): 1-12.

Kelsey, Jeffrey. “Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.” *Michigan Law Review* 106 (May 2008): 1427-52.

Korns, Stephen, and Joshua E. Kastenberg. “Georgia’s Cyber Left Hook.” *Parameters* 38 (Winter 2008-09): 61-76.

McCullough, Bernard J. III. “Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations, U.S. Fleet Cyber Command.” *Congressional Record* (September 23, 2010): 1-9.

Menn, Joseph. "Rules of Engagement for Cyberwars See Slow Progress." *Financial Times* (December 29, 2010): 4. http://www.proquest.com.ezproxy. library.tufts.edu (accessed January 13, 2011).

Miranda, Kay. “Definition of Code of Conduct.” http://www.ehow.com/about_ 5044074 _ definition- code-conduct.html#ixzz1AwsrUmtS (accessed January 13, 2011).

National Research Council of the National Academies. *Proceedings of a Workshop On Deterring Cyberattacks: Informing Strategies and Developing Options For U.S. Policy*. Washington, DC: The National Academies Press, 2010.

National Security Council. “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.” The White House. http://www.whitehouse.gov/CyberReview (accessed November 8, 2010).

Obama, Barack H. *National Security Strategy.* Washington, DC: The White House, May 2010.

"Rules of Engagement." *The Oxford Essential Dictionary of the U.S. Military.* New York, NY: Berkley Books, 2001. http://www.oxfordreference.com.ezproxy.library.tufts.edu/views/ ENTRY.html?subview=Main&entry=t63.e6938 (accessed January 13, 2011).

Smith, Steven. "Defending the Nation Against Cyber Attack." Lecture, The Fletcher School of Law and Diplomacy, International Security Studies Program Luncheon, Medford, MA, October 18, 2010. Cited with permission of Steven Smith.

U.S. Air Force. *Cyberspace Operations.* Air Force Doctrine Document 3-12. Washington, DC: Secretary of the Air Force, July 15, 2010.

U.S. Department of the Army. *Information Security Program,* Army Regulation 380-5. Washington, DC: U.S. Department of the Army, September 29, 2000.

U.S. Department of the Army. *Information Systems Security,* Army Regulation 380-19. Washington, DC: U.S. Department of the Army, February 27, 1998.

U.S. Department of the Navy. *Information Security Program*. Secretary of the Navy M-5510.36. Washington, DC: Chief of Naval Operations, June 30, 2006.

U.S. Department of the Navy. *Information Systems Security Program.* Bureau of Naval Personnel Instruction 5239.1B. Millington, TN: Chief of Naval Personnel, April 5, 2001.

Vatis, Michael. "The Next Battlefield: The Reality of Virtual Threats." *Harvard International Review* 28, no. 3 (Fall 2006): 56-61.

Washington, Ollie. *The Legal and Ethical Implications of Information Operations.* Strategy Research Project. Carlisle Barracks, PA: U.S. Army War College, April 10, 2001.

Webber, Richard E. "Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations, U.S. Air Force Cyber Command." *Congressional Record* (September 23, 2010): 1-10.